UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,124	11/25/2003	Masaaki Takase	FUJY 20.758	9438

26304 7590 12/26/2007

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	10/723,124	TAKASE ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 10/5/2007, Applicant amends claims 2, 8, 9, and 10. The following claims 1-16 are presented for examination.

1.1 In response to communications filed on 10/5/2007, the 112th rejection of claim 10 has been withdrawn in view of the amendment. However, the 112th rejection with respect to the other claims 2, 8, and 9 has not been withdrawn as explained further below.

1.2 Applicant's arguments, pages 8-10, filed on 10/5/2007 have been fully considered but they are not persuasive. With regard to claim 1, Applicant states that in Anzai the decode key A and the reserve key B are not used at the same time. Examiner respectfully disagrees as the claim does not require the keys to be used at the same time. Also applicant is referring to an embodiment (paragraphs 86-87) that is not used in the rejection to show that the decode key A is discarded whereas Applicant's specification uses an embodiment for discarding the old key (see Applicant's specification, paragraphs 91, 136, and 151). Applicant adds that the reserve key B is used in exchange and not used as a decode key in paragraphs 86-87. Examiner respectfully disagrees as Anzai discloses in paragraph 87 "Encryption C is received and it decrypts with the decode key B". Examiner asserts that Anzai discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 and page 2, paragraph 17) and further discloses (page 2, paragraph 24 and claim 2) that the sending station has means for decrypting encryption

data from the receiving station using the cryptography key; the reserve key is also used for encryption/decryption because after updating, the reserve key is made into a new key (see page 3, paragraph 20) that meets the recitation of first setting unit setting *a most-updated encryption key* (reserve key or new key) *and a one-generation-anterior encryption key* (cryptographic key) *for receipt, respectively.* Anzai also discloses the receiving station decrypting an encrypted reserve key using a decode key (for receipt) and the reserve key now is set as the new decode key which decrypts encryption data (for receipt) (see paragraphs 20-21 and 23-24) that meets the claimed limitation of *a second setting unit setting a most-updated encryption key and a one-generation-anterior key for receipt, respectively.* Therefore, applicant has not overcome the rejection of claim 1 and the claim remains rejected in view of Anzai. No further arguments were presented by applicant regarding claims 2-16. Therefore claims 2-16 are not overcome by Applicant for the same reasons given above with respect to claim 1.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 2, 8, 9, and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

2.1 Regarding claims 2, 8, and 9 the claims recite the limitation "...acquisition unit which is used to acquire all of the encryption keys..." and "the encryption key acquired". However,

different encryption keys are cited and it is not clear which encryption key is being claimed. There is insufficient antecedent basis for this limitation in the claims. It is also noted that the specification uses "singular form" in describing acquisition unit acquiring encryption key. Other claims depending directly or indirectly from claims 2, 8, and 9 recite similar limitations.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-11 and 14-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Japanese Patent Publication 11-196081 published on (July 21, 1999) to **Anzai**.

As per claim 1, **Anzai** discloses in a system for performing encryption communications using a common key updated at a predetermined timing between a key transmitting device and a key receiving device, a common key encryption communication system comprising: *a key transmitting device* (sending station) *including first retaining unit* (storage means in sending station) *retaining a most-updated encryption key* (reserve key or new key) *and a one-generation-anterior encryption key* (cryptographic key) *as the above common keys* (see page 4, paragraph 23), and **Anzai** discloses means for using the cryptographic key (one-generation-anterior

encryption key) for encrypting data for delivery or transmission that meets the recitation of *a first setting unit setting a one-generation-anterior encryption key for transmission* (see page 3, paragraph 20). **Anzai** also discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 and page 2, paragraph 17) and further discloses (page 2, paragraph 24 and claim 2) that the sending station has means for decrypting encryption data from the receiving station using the cryptography key; the reserve key is also used for encryption/decryption because after updating, the reserve key is made into a new key (see page 3, paragraph 20) that meets the recitation of setting *a most-updated encryption key* (reserve key or new key) *and a one-generation-anterior encryption key* (cryptographic key) *for receipt, respectively*; *and the above key receiving device* (receiving station) *including second retaining unit* (storage means in receiving station) *retaining a most-updated encryption key* (reserve key) *and a one-generation-anterior encryption key* (previous decode key) *as the above common keys*, (see page 4, paragraph 23); and **Anzai** discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 page 4, paragraph 23), **Anzai** also discloses means for using the reserve key (most-updated encryption key) as a new decode key and the decode key may be used for encrypting data for delivery or transmission that meets the recitation of *a second setting unit setting a most-updated encryption key for transmission* (see page 4, paragraphs 23-24), **Anzai** further discloses (page 4, paragraph 24 and claim 2) that the receiving station has means for decrypting encryption data from the sending station using the decode key; the reserve key is also used for encryption/decryption because after updating, the reserve key is made into a new decode key (see page 3, paragraph 23) that meets the recitation of *a most-updated encryption key and a one-generation-anterior key for receipt, respectively.*

As per claim 2, **Anzai** discloses updating and storing the cryptographic key making the reserve key becoming a new cryptographic key and further discloses a reserve key acquired becomes the new reserve key (see page 8, paragraphs 58-62) that meets the recitation of wherein the above key transmitting device further includes acquisition unit which is used to acquire all of the encryption keys, the above first retaining unit updates and retains the above most-updated encryption key (reserve key) as the one-generation-anterior encryption key and the encryption key acquired by the above acquisition unit as the most-updated encryption key, respectively, and further discloses the keys after updating are set for transmission and receipt in the sending station as explained in the rejection of claim 1 above (see pages 3-4, paragraphs 22-24) that meets the recitation of the above first setting unit re-sets the one-generation-anterior encryption key for transmission, and the most-updated encryption key and the one-generation-anterior encryption key for receipt respectively on the basis of the retained key after being updated by the above first retaining unit.

As per claim 3, **Anzai** discloses the limitation of wherein the above key transmitting device includes generation unit generating the encryption key, and the above acquisition unit acquires the encryption key generated by the above generation unit (see page 8, paragraphs 60-61).

As per claim 4, **Anzai** discloses the limitation of wherein the above key transmitting device further includes first transmitting unit transmitting the encryption key acquired by the above acquisition unit to the key receiving device (see page 8, paragraphs 62-63).

As per claim 5, **Anzai** discloses wherein the above key receiving device further includes second receiving unit receiving the encryption key transmitted from the above key transmitting device (see page 8, paragraphs 70-71), **Anzai** discloses updating and storing the reserve key making the reserve key becoming a new decode key and further discloses a reserve key acquired becomes the new reserve key into a new reserve key (see page 8, paragraphs 70-73) that meets the recitation of in case the above second receiving unit receives the encryption key, the above second retaining unit respectively updates and retains the above most-updated encryption key as the one-generation-anterior encryption key and the encryption key received by the above second receiving unit as the most-updated encryption key, and further discloses the keys after updating are set for transmission and receipt in the receiving station as explained in the rejection of claim 1 above (see pages 3-4, paragraphs 22-24) that meets the recitation of the above second setting unit respectively re-sets the most-updated encryption key for transmission, and the most-updated encryption key and the one-generation-anterior encryption key for receipt on the basis of the retained key after being updated by the above second retaining unit.

As per claim 6, **Anzai** discloses the limitation of wherein the above key receiving device includes second transmitting unit transmitting a predetermined message to the key transmitting device, and the above key transmitting device includes first receiving unit receiving the

predetermined message transmitted from the above key receiving device (see page 4, paragraph 24).

As per claim 7, **Anzai** discloses the limitation of wherein the above first and second retaining unit respectively retain the initialization key (see page 8, paragraphs 58 and 68 and see page 9, paragraphs 78 and 85).

As per claim 8, **Anzai** discloses combining the conventional system with the invention, the conventional system wherein an updating demand is performed to update from the receiving station to the sending station (see pages 1-2, paragraphs 3 and 9) that meets the recitation of wherein the above key receiving device transmits a key initialization request message as the above predetermined message at a predetermined timing, in case the above key transmitting device receives the key initialization request message transmitted from the above key receiving device; and **Anzai** further discloses the above acquisition unit is used to acquire all of the encryption keys, and the above first retaining unit respectively updates and retains the common initialization key as the one-generation-anterior encryption key and the encryption key acquired by the above acquisition unit as the most-updated encryption key (see page 8, paragraphs 58-62).

As per claim 9, **Anzai** discloses combining the conventional system with the invention, the conventional system wherein an updating demand is performed to update from the receiving station to the sending station (see pages 1-2, paragraphs 3 and 9) that meets the recitation of wherein the above key receiving device transmits a key update request message as the above

predetermined message at a predetermined timing, in case the above key transmitting device receives a key update request message transmitted from the above key receiving device; and **Anzai** further discloses the above acquisition unit is used to acquire all of the encryption keys, and the above first retaining unit respectively updates and retains the above common initialization key as the one-generation-anterior encryption key and the encryption key acquired by the above acquisition unit as the most-updated encryption key (see page 8, paragraphs 70-73).

As per claim 10, **Anzai** discloses wherein the above key receiving device includes unit determining a key update timing (see claim 4), and said second transmitting unit transmitting a predetermined message to the key transmitting device, (see page 4, paragraph 24), in the case of reaching the key update timing, transmits the key update request message to the key transmitting device (see page 1, paragraph 3).

As per claim 11, **Anzai** discloses wherein the above key transmitting device includes unit determining a key update timing, and said first transmitting unit, in the case of reaching the key update timing, transmits the encryption key acquired by the above acquisition unit to the key receiving device (see page 8, paragraphs 56-59).

As per claim 14, **Anzai** discloses in a key transmitting device performing encryption communications using a common key updated at a predetermined timing with a key receiving device, a key transmitting device comprising *retaining unit* (storage means in sending station)

retaining a most-updated encryption key (reserve key or new key) *and a one-generation-anterior encryption key* (cryptographic key) *as the above common keys* (see page 4, paragraph 23), and **Anzai** discloses means for using the cryptographic key (one-generation-anterior encryption key) for encrypting data for delivery or transmission that meets the recitation of *setting unit respectively setting a one-generation-anterior encryption key for transmission* (see page 3, paragraph 20). **Anzai** also discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 and page 2, paragraph 17) and further discloses (page 2, paragraph 24 and claim 2) that the sending station has means for decrypting encryption data from the receiving station using the cryptography key; the reserve key is also used for encryption/decryption because after updating, the reserve key is made into a new key (see page 3, paragraph 20) that meets the recitation of setting *a most-updated encryption key* (reserve key or new key) *and a one-generation-anterior encryption key* (cryptographic key) *for receipt.*

As per claim 15, **Anzai** discloses in a key receiving device performing encryption communications using a common key updated at a predetermined timing with a key transmitting device, a key receiving device comprising *retaining unit* (storage means in receiving station) *retaining a most-updated encryption key* (reserve key) *and a one-generation-anterior encryption key* (previous decode key) *as the above common keys*, (see page 4, paragraph 23); and **Anzai** discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 page 4, paragraph 23), **Anzai** also discloses means for using the reserve key (most-updated encryption key) as a new decode key and the decode key may be used for encrypting data for delivery or transmission that meets the recitation of *setting unit setting a most-updated*

encryption key for transmission (see page 4, paragraphs 23-24), **Anzai** further discloses (page 4, paragraph 24 and claim 2) that the receiving station has means for decrypting encryption data from the sending station using the decode key; the reserve key is also used for encryption/decryption because after updating, the reserve key is made into a new decode key (see page 3, paragraph 23) that meets the recitation of *a most-updated encryption key and a one-generation-anterior key for receipt, respectively.*

As per claim 16, **Anzai** discloses in a method of performing encryption communications using a common key updated at a predetermined timing between a key transmitting device and a key receiving device, a common key encryption communication method characterized in that *the key transmitting device* (sending station) *retains a most-updated encryption key* (reserve key or new key) *and a one-generation-anterior encryption key* (cryptographic key) *as the above common keys,* (see page 4, paragraph 23), and **Anzai** discloses means for using the cryptographic key (one-generation-anterior encryption key) for encrypting data for delivery or transmission. **Anzai** also discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 and page 2, paragraph 17) that meets the recitation of *sets respectively the one-generation-anterior encryption key for transmission and for receipt, and the above key receiving device* (receiving station) *retains the most-updated encryption key* (reserve key) *and the one-generation-anterior encryption key* (previous decode key) *as the above common keys*, (see page 4, paragraph 23); and **Anzai** discloses common key cryptography used for encryption/decryption (see page 1, paragraph 1 page 4, paragraph 23), **Anzai** also discloses means for using the reserve key (most-updated encryption key) as a new decode key and the

decode key may be used for encrypting data for delivery or transmission that meets the recitation of *and sets respectively the most-updated encryption key for transmission* (see page 4, paragraphs 23-24), **Anzai** further discloses (page 4, paragraph 24 and claim 2) that the receiving station has means for decrypting encryption data from the sending station using the decode key; the reserve key is also used for encryption/decryption because after updating, the reserve key is made into a new decode key (see page 3, paragraph 23) that meets the recitation of *a most-updated encryption key and a one-generation-anterior key for receipt.*

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Japanese Patent Publication 11-196081 published on (July 21, 1999) to **Anzai** in view of US Patent 7,024,553 to **Morimoto**.

As per claim 12, **Anzai** substantially teaches the claimed system of claim 4. **Anzai** further discloses in drawing 4 in combination with paragraphs 65-67, restarting the process wherein received data have been sent as an input if not equal. **Anzai** is silent about the request is resent to the transmitting device. It is apparent that received data may have been sent (paragraph 65) as an updating demand by the receiving device as suggested in paragraph 3. **Morimoto** in an analogous art teaches key request message between two devices for authentication purpose (see column 10, lines 45-56) and further discloses key resending request message at a predetermined timing to provide for compatibility of high management performance and high information confidentiality (see column 12, lines 4-44) (see also column 14, lines 5-12 and figure 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Anzai** to include key notification message as taught by **Morimoto** so as to verify the party making the request and key synchronization can take place when there is lack of coincidence (see **Morimoto** column 13, lines 24-37).

5. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over Japanese Patent Publication 11-196081 published on (July 21, 1999) to **Anzai**.

As per claim 13, **Anzai** substantially teaches the claimed system of claim 4. **Anzai** also discloses initialization value to update keys (see paragraph 78). **Anzai** discloses discarding the previous key (see paragraphs 80 and 82), but is silent about retaining none of the keys. It is a well-known practice in the art that keys may be discarded after use to prevent tampering. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the system of **Anzai** to retain none of the keys because updating would be able to perform from initialization key value while none of the keys would be retained to prevent tampering.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses key synchronization and key update. (See PTO-form 892).

6.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/

Carl Colin
Patent Examiner, A.U. 2136
December 14, 2007